REMARKS

The Application has been carefully reviewed in light of the Office Action dated December 14, 2006. Claims 1-17 are currently pending in the application, with Claims 1-3 and 14-17 having been amended. Reconsideration and further examination is respectfully requested.

Rejections under 35 USC § 112

Claims 1-17 have been rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, the Office Action states that the recitation "outputting the update calculation result c for each of the values {f_i} as x^e, is misdescriptive as if each of the updated calculation result c for each of the values {f_i} is output as x^e.

Amended independent Claim 1 is directed to an exponent calculation apparatus for calculating x^e based on two integers x and e, the apparatus comprising, an input unit for inputting the two integers x and e, a candidate exponents storing unit for storing candidate exponents {l_i} (0≤i≤L-1), the number of the candidate exponents being L, a pre-calculation unit for pre-calculating x^{l_i} for each of the candidate exponents {l_i}, which are stored in the candidate exponents storing unit, based on the input integer x, a pre-calculated values storing unit for storing the values x^{l_i} obtained by the pre-calculation, a dividing unit for dividing the input integer e into a plurality of values {f_i} (0≤i≤F-1) so that each of the values {f_i} corresponds to one of the candidate exponents {l_i}, a calculation result storing unit for storing a calculation result c, a sequential processing unit for sequentially updating the calculation result c for each of the divided values {f_i} (0≤i≤F-1) by using each of the pre-calculated values x^{l_i}, and an output unit for outputting the calculation result c as x^e after the calculation result c is updated for all the values {f_i} as x^e.

Independent Claim 1 has been amended to provide further clarification to what is being outputted, specifically, an output unit for outputting the calculation result c as x^e after the calculation result c is updated for all the values {f_i} as x^e. Amended independent Claim 1 is therefore believed to be in condition for allowance, and such action is respectfully requested. In addition, amended independent Claims 2, 14, 15, 16, and 17 are claims that contain substantially similar features as that of amended independent Claim 1, and are therefore also believed to be in condition for allowance for at least the reasons discussed above with respect to amended independent Claim 1.

Turning to the rejection of dependent Claim 3, the Office Action states that the recitation, "updating bit length represented by $c:=c^2$", is unclear. Dependent Claim 3 has been amended to provide further clarification, specifically, amended dependent Claim 3 is directed to an updating unit for sequentially updating $c:=c^2$ as many times as a number of a bit length of each of the divided values {f_i} ($0 \leq i \leq F-1$) in binary notation and updating c:=c*f_i. Hence, reconsideration and withdrawal of the claim rejection is respectfully requested.

Rejections under 35 USC § 101

Claims 14-17 have been rejected under 35 USC § 101 as allegedly directed to non-statutory subject matters.

Amended independent Claim 14 is directed to a method for encrypting or decrypting data by calculating x^e based on two integers x and e. In this regard, the present invention of independent Claim 14 recites a practical purpose, which is encrypting and decrypting data. Therefore, Claim 14 is believed to be in condition for allowance, and such action is respectfully requested. In addition, independent Claim 15 contains substantially similar features as that of independent Claim 14, and is therefore also believed to be in condition for allowance for at least the reasons discussed above with respect to independent Claim 14.

Turning to amended independent claims 16 and 17, amended independent Claims 16 and 17 are directed to computer-readable programs stored in computer-readable storage mediums. Hence, Claims 16 and 17 are believed to be in condition for allowance, and such action is respectfully requested.

CONCLUSION

Applicant respectfully submits that all of the claims pending in the application meet the requirements for patentability and respectfully requests that the Examiner indicate the allowance of such claims.

Any amendments to the claims which have been made in this response which have not been specifically noted to overcome a rejection based upon prior art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

Should the Examiner have any questions, the Examiner may contact Applicant's representative at the telephone number below.

Respectfully submitted,

3/13/07

Date

/Trevor Chuang/

Trevor Chuang, Reg. No. 55,073
Patent Agent for Applicant

Canon U.S.A. Inc., Intellectual Property Division
15975 Alton Parkway
Irvine, CA 92618-3731
Telephone: (949) 932-3310
Fax: (949) 932-3560